汉坤法律评述
漢坤律師事務所
融贯中西 · 务实创新
2018 年 7 月 14 日

汉坤网络安全和数据合规系列之九：DPO 职位，你敢不敢？

朱敏

网络安全和数据合规，是眼下许多公司法务和合规部门朋友讨论的热门话题，在讨论技术性问题之余，我们今天换个思路，来谈谈跟数据业务部门或岗位关系更加密切的“数据保护官（DPO）”的话题。

2018 年 5 月底，国内某航空公司正式任命其总法律顾问为公司数据保护官，全面负责企业的数据保护与合规运营工作，成为国内首家设立数据保护官的企业。据 7 月 8 日新华社微博“新华视点”发布的山东省近日破获的一起特大侵犯公民个人信息案，11 家涉案公司中有 3 家涉嫌单位犯罪，不仅因数据不合规而陷入刑事责任，更在单位犯罪的双罚制下，其法定代表人和相关数据主管人员也难逃刑事责任之虞。

隐藏在 DPO 话题下的不仅是对数据合规的需求，也有对 DPO 和公司的职责和风险之辩：DPO 职位究竟指向什么？企业设立 DPO 是否满足了现行法的要求？DPO 能否对标中国法语境下的网络安全负责人、个人信息保护负责人和首席数据官等？它的具体职责是什么？履行职责过程中是否会有任何法律责任风险，尤其是个人责任？

一、 DPO 究竟是什么职位？

GDPR 首次以法律形式明确规定 DPO 的职责，但并未对 DPO 作出明确的定义。结合 GDPR 项下 DPO 的地位和职责，我们认为 DPO 可被描述为以独立的立场和方式确保 GDPR 在数据控制者和数据处理者中的适用，监督数据控制者和数据处理者的数据合规，并协助监管机构执法的专业人员。

GDPR 项下的 DPO，在一定程度上担当着监管机构和数据控制者之间的桥梁角色，一方面协助数据控制者评估数据处理的风险，另一方面在数据控制者违规或存在违规风险时提出整改建议，并在发生数据泄露事件时作为监管机构和数据控制者的联络人。[1]也正因为其特殊的中间地位，数据控制者在任命 DPO 时，独立性是必须考量的因素。

在我国现行法中，和 DPO 可能对标的有《网络安全法》、《关键信息基础设施安全保护条例（征求意见稿）》（“**《CII 条例》**”）、《网络安全等级保护条例（征求意见稿）》（“**《等保条例》**”）、《公安机关互联网安全监督检查规定（征求意见稿）》中提及的网络安全（管理）负责人、《信息安全

[1] GDPR, Art. 33.3(b).

技术 个人信息安全规范》（“**《安全规范》**”）中提及的个人信息保护负责人以及《银行业金融机构数据治理指引》确定的首席数据官。其中首席数据官一职在《指引》下由银行自愿设立，且《指引》和《中国银监会中资商业银行行政许可事项实施办法》对首席数据官的任职资质提出了行政许可的要求[2]。网络安全负责人和个人信息保护负责人在设立目的上和 DPO 存在相似性，都为个人信息保护和隐私数据合规而生，这从下文有关其职位职责的讨论中可以得到印证。

二、 企业是否必须任命 DPO？

DPO 的设立目的之一在于个人信息保护，蕴含着公共利益属性。因此，各国法律及相应指南[3]在某些特殊领域和达到一定规模的数据处理上，往往要求数据控制者强制设立 DPO，以防范个人信息被侵害的风险。以 GDPR 为例，在下列情形中应当任命 DPO：（1）数据处理由公权力部门或机构实施（司法机关除外）；（2）数据控制、处理者的核心业务活动包括对数据主体进行大规模系统化监控；（3）数据控制者和数据处理者的大规模数据处理涉及个人特殊类型数据（如民族、宗教、政治观点、性取向等敏感数据）和犯罪数据[4]。

而《网络安全法》的强制设立义务针对所有的网络运营者，要求任何网络运营者都要按照网络安全等级保护制度的要求，确定网络安全负责人。根据《等保条例》，网络以私主体利益、公共利益和国家安全三个标准被分为五个安全保护等级，即便是第一级等保评级，《等保条例》也明确要求网络运营者设立网络安全负责人，不同保护等级的网络运营者中的网络安全负责人只在安全背景审查和责任承担上有所区别[5]。《网络安全法》和《CII 条例》则要求 CII 运营者应“设置专门网络安全管理机构和网络安全管理负责人，并对该负责人和关键岗位人员进行安全背景审查”[6]。

《安全规范》则以规模标准提出对个人信息保护负责人专职的要求，即在以下情形中个人信息控制者应当设置专职的个人信息保护负责人：（1）主要业务涉及个人信息处理，且从业人员规模大于 200 人；（2）处理超过 50 万人的个人信息，或在 12 个月内预计处理超过 50 万人的个人信息[7]。此时，个人信息保护负责人不能由企业内部其他职能部门的人员兼任。

通过上述比较，我们发现数据规模、类型和领域等是强制设立 DPO 义务的几个主要界定标准。GDPR 以“核心业务+特殊领域+抽象的规模性”为限定，看似在相当范围内排除了强制设立 DPO 的义务。而《网络安全法》、《等保条例》和《CII 条例》则采取了“强制设立为基础+权益侵害加重”的模式，看似涉及范围最大。《安全规范》则以具体的规模标准来确定专职保护负责人的设立义务，也对一般的保护负责人的设立提出了普遍要求。

---

[2] 《银行业金融机构数据治理指引》第十一条：银行业金融机构可根据实际情况设立首席数据官。首席数据官是否纳入高级管理人员由银行业金融机构根据经营状况确定；纳入高级管理人员管理的，应当符合相关行政许可事项的要求；《中国银监会中资商业银行行政许可事项实施办法》第七十八条：中资商业银行行长、副行长、行长助理、风险总监、合规总监、总审计师、总会计师、首席信息官以及同职级高级管理人员，内审部门、财务部门负责人，总行营业部总经理（主任）、副总经理（副主任）、总经理助理，分行行长、副行长、行长助理，分行级专营机构总经理、副总经理、总经理助理，分行营业部负责人，管理型支行行长、专营机构分支机构负责人等高级管理人员，须经任职资格许可。

[3] 如 GDPR Art. 37、德国《数据保护法》（Data Protection Act）第 4（f）条和《等保条例》第二十一条。

[4] GDPR, Art. 37.1.

[5] 《等保条例》第二十条和第二十一条。

[6] 《网络安全法》第三十四条之一和《CII 条例》第二十四条。

[7] 《安全规范》第 10.1（b）条。

但表面上的限制和排除要件的比较并不能简单得出强制设立义务的轻重差异，在考量具体规定的适用力度时，还需要结合条文的适用场景和相对应的法律后果。事实上，正因为 GDPR 采用了“规模性”这一抽象的标准，在解释上往往可能纳入更多的适用情形。正如欧盟第 29 条数据保护工作组（“**WP29**”）在《DPO 指南》中所指出，以一个明确的数字规模标准来判断应当设立 DPO 的所有情形并不现实。相反，采取抽象的标准不会排除某些应该适用规范的可能情形。根据 WP29 的建议，涉及的数据主体数量、数据处理的体量、不同数据项下的范围、数据处理的存续期间和保持期间、数据处理的地理范围等因素，都是判断规模较大的标准[8]。相较之下，采用确定的数字规模标准反而可能会遗落部分体量不足，但领域较为敏感的数据处理活动。

在违反强制设立义务的责任承担上，GDPR 以绝对优势的处罚力度胜过国内相关规定。依据 GDPR 第 83.4（a）条之规定，数据控制者或者处理者需要支付 10,000,000 欧元和企业上一财务年度全球营业总额 2%中的较高者的行政罚款。而《网络安全法》、《等保条例》和《CII 条例》所规定的处罚力度则要小得多。在网络运营者未尽到强制设立义务之时，仅由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款[9]。其中，CII 运营者和等保评估三级及以上的网络运营者按照规定从重处罚[10]。而《安全规范》作为国家推荐标准，本身并无强制执行力，标准中也未有法律后果的规定。因此，在强制设立义务上，GDPR 在目前应是最为严格的规定。

三、 DPO 的义务和职责是什么？

个人信息保护和数据合规是 GDPR 项下 DPO 的设立目的，我国对标的网络安全负责人还纳入了网络主权和国家安全等立法预设目的。目的决定职责范围，而职责的轻重又影响到法律风险的高低。因此，讨论 DPO 的职责其实一定程度上也是在明确 DPO 可能的法律风险。

首先需要明确的是，无论在哪一个法律文件项下，DPO 都不是最上位的数据保护责任者。GDPR 中，DPO 的上位责任者为数据控制者和数据处理者，《网络安全法》中网络安全负责人的上位责任者为网络运营者，《安全规范》中个人信息保护责任人的上位责任者是个人信息控制者。

而在具体职责上，GDPR 在上位责任者的职责范围之外明确规定了 DPO 的详细职责：（1）为数据处理者、数据控制者及相关数据处理人员提供信息和建议；（2）监督 GDPR、成员国数据法规、数据控制者和处理者政策的合规性；（3）提供有关数据保护影响评估的建议；（4）同监管机构协作；（5）为监管机构和数据处理活动提供联络[11]。

根据 GDPR 第 38 条的规定和《DPO 指南》对 DPO 职责的解读，其职责范围被表述为“参与和个人数据保护相关的所有事项”，[12]以及“及于数据控制者和数据处理者所有的数据处理活动”[13]。这意味着 DPO 对数据合规的审查职责是全流程的，在数据影响评估的最早阶段，DPO 即有义务介入流程。此外，日常的数据处理活动，DPO 也有监管职责。一言以蔽之，GDPR 项下的 DPO 的职责范

[8] WP 243 rev.01 Guidelines on Data Protection Officers, p7-8.

[9] 《网络安全法》第二十一条。

[10] 《CII 条例》第四十五条和《等保条例》第六十三条。

[11] GDPR, Art. 39.1.

[12] GDPR, Art. 38.1 and WP 243 rev.01 Guidelines on Data Protection Officers, Section 3 “Position of the DPO”.

[13] “……is for all the processing operations carried out by the controller or the processor”, WP 243 rev.01 Guidelines on Data Protection Officers, p6.

围涉及数据合规的所有方面。

《安全规范》将个人信息保护负责人和个人信息保护工作机构应履行的职责概括为：（1）全面统筹实施组织内部的个人信息安全工作，对个人信息安全负直接责任；（2）制定、签发、实施、定期更新隐私政策和相关规程；（3）建立、维护和更新组织所持有的个人信息清单（包括个人信息的类型、数量、来源、接收方等）和授权访问策略；（4）开展个人信息安全影响评估；（5）组织开展个人信息安全培训；（6）在产品或服务上线发布前进行监测，避免未知的个人信息收集、使用共享等处理行为；（7）进行安全审计等。

而《网络安全法》则并未对网络安全负责人的具体职责和网络运营者进行区分界定。通过上述比较，我们可以看出，GDPR 项下的 DPO 的职责范围被明确要求为全流程和全事项，《网络安全法》并没有区分网络安全负责人和上位责任人的职责范围，仅规定了上位责任人的安全保护义务，而《安全规范》则以较为笼统的概括性规定描述了个人信息保护负责人的职责范围。

那么是否意味着，职责范围无比巨大的 DPO，在法律风险上比未明晰职责的网络安全负责人和个人信息保护负责人要大得多呢？结论可能恰恰相反。理论上来说，GDPR 框架下 DPO 的法律责任和风险比国内的网络安全负责人和个人信息保护负责人可能反而要小。

四、 DPO 职位有法律风险吗？

为何 GDPR 语境下的 DPO 其法律风险小于中国法语境下的网络安全负责人等职位？其原因在于 GDPR 项下的 DPO 的个人责任原则上被机构责任所吸收，只在职位独立性受到影响和 DPO 不尽职时才有承担个人责任的法律风险。而中国法下的网络安全负责人等职位同机构绑定，个人责任的承担为原则性规定，法律风险相对反而较大。

GDPR 第 24 条“控制者责任”中明确了数据控制者对数据合规负责的原则，第八章“救济、责任和处罚”一章中的规制主体也基本都指向了数据控制者和处理者。WP29 更是在《DPO 指南》中明确地指出 DPO 对数据的不合规不负个人责任，应且只应当是数据控制者才负有确保数据合规的义务[14]。这一特殊的责任制度设计，目的在于尽可能的维持 DPO 的独立性，让 DPO 不受数据控制者的不当辖制，更好的行使监督职能。由此，DPO 的风险之一是在公司内部人员兼任时（Internal DPO），因职责和利益冲突，DPO 任职者可能被定性为数据控制者的组成部分，从而承担相应的法律责任；风险之二则由 GDPR 第 38 条“尽职豁免”规定的反面解释推导而来，DPO 只能在不尽职之时受到解雇和其他相关的处罚[15]。

如果说 GDPR 项下的 DPO 责任承担以机构责任为原则，个人责任为例外，那么我国的网络安全负责人等职位，虽无法律规定的具体职责范围和法律责任，但因企业不合规行为的责任双轨制，可能存在着潜在的个人责任风险。

《网络安全法》在“法律责任”一章的各项条款中，均规定在出现违法行为时，除对单位课以处罚之外，直接负责的主管人员和其他责任人员也应承担相应的行政责任。《刑法》也在第二百五十三条之一“侵犯公民个人信息罪”和第二百八十六条“拒不履行信息网络安全管理义务罪”中明确了

[14] GDPR, Art. 24.1; WP 243 rev.01 Guidelines on Data Protection Officers, p17.

[15] GDPR, Art. 38.3：数据控制者和处理者应当确保数据保护专员不会收到任何有关执行其工作任务的指示。他或她不能因执行自身的任务而被解雇或处罚。数据保护专员应当直接向数据控制者或处理者的最高管理层报告。

构成单位犯罪的直接负责的主管人员和其他直接责任人员的刑事责任。不过，从目前的行政执法和刑事司法实践来看，被处罚的行为均具有明显的不法性，典型行为如非法窃取和泄漏数据或者以营利为目的的数据出售行为等，我们也相信因合法的业务行为而遭受严厉行政制裁尤其是入罪的可能性应该不大。

关于如何认定“直接负责的主管人员和其他直接责任人员”，值得所有从事数据相关业务的小伙伴们注意。按最高法的口径：直接负责的主管人员，是在单位实施的犯罪中起决定、批准、授意、纵容、指挥等作用的人员，一般是单位的主管负责人，包括法定代表人。其他直接责任人员，是在单位犯罪中具体实施犯罪并起较大作用的人员，既可以是单位的经营管理人员，也可以是单位的职工，包括聘任、雇佣的人员。应当注意的是，在单位犯罪中，对于受单位领导指派或奉命而参与实施了一定犯罪行为的人员，一般不宜作为直接责任人员追究刑事责任[16]。

附表:各项法律下 DPO 及类似职位比较：

法规	职位名称	职责范围	上位责任人	责任形式	承担责任方式	豁免机制
GDPR	DPO	全流程、全事项	数据处理者	机构责任	解雇和处罚（处罚未明确规定）	尽职豁免
网络安全法	网安负责人	未规定	网络运营者	个人责任和机构责任	民事、行政、刑事责任	无
个人信息安全规范	个人信息保护负责人	概况性规定	个人信息控制者	个人责任和机构责任	民事、行政、刑事责任	无

五、 网络安全负责人，该何去何从？

在《网络安全法》和《安全规范》相继颁布后，网络安全负责人和个人信息保护负责人已然是相关企业不得不设立的职位。但在中国法语境下的这两者和 GDPR 项下的 DPO 并不能完全对标，在责任承担上也呈现出一定的个人化和刑事化趋势。如果制度设计和责任分配失当，则无疑会降低任职人员的任职动力，出现无人愿意担任网络安全负责人或个人信息保护负责人的尴尬局面，这不仅不利于企业的数据处理业务发展，也会让《网络安全法》等法律维护网络安全、保护个人信息、促进数据合规等立法目的落空。

因此，我们认为，应提高对网络安全负责人和个人信息保护负责人的风险防范和制度保护，减轻他们的不合理的责任负担。具体而言，可从以下几方面予以考虑：

(一) 建立尽职豁免机制，弱化责任个人化趋势

GDPR 项下的 DPO 以机构责任为原则，个人责任被豁免，且为了 DPO 职责的更好行使，DPO 的尽职豁免解雇制度让 DPO 最大限度的不受数据控制者的不当辖制。而在现行中国法下，并没有明确机构责任为原则，个人责任也没有很直接的保护和豁免机制。故在个人责任的承担上应当考虑适当的尽职豁免制度，弱化责任个人化的绝对承担。不过，如前所述，在现阶段的执法环境中，除非在数据业务岗位上直接参与或从事明显的不法行为或存在重大的过失行为，个人在正常

[16] 《最高人民法院关于印发<全国法院审理金融犯罪案件工作座谈会纪要>的通知》（法〔2001〕8 号）第（一）2 条。

的业务行为过程中并不具备被轻易追责的风险因素。

(二) 民事责任先行，防止刑民越界造成责任失衡

当前，在个人信息保护领域的法律体系建设上，存在明显的刑强民弱趋势，这不仅是因为民事立法的相对滞后，也和刑事司法的强势和扩张有一定的关联。但在不少实践场景中，不同业务主体之间交换或共享个人信息数据，民事或者行政救济已然足够并能更为合理地保护被侵权人的权益。因为民事救济中，允许司法裁量在个人尊严和自由的法益（个人利益）与个人信息自由流通（公共利益）加以衡量，作出恰当的责任分配[17]。网络运营者及其网络安全负责人的责任刑事化应在民事救济已然穷尽并不足以保护被侵害人时才具有正当性。

(三) 建立任职资质要求，做好事先风险防范

虽然 GDPR 本身并未对 DPO 的任职资质做出具体要求，但 WP29 建议 DPO 应熟悉欧盟及成员国数据保护法律，并对 GDPR 有足够深刻的了解和相关任职经验，而在公共机构任职的 DPO，还应当对机构的运营章程和程序有较深的了解[18]。因此 DPO 的资质要求因其任职的特殊领域会有所提高。《网络安全法》则并未对网络安全负责人做出相应的资质要求，《等保条例》只表明应对等保三级以上的网络运营者的网络安全负责人进行安全背景审查。但我们认为确立资质要求有助于确保该职位从业人员的素质，做好事先风险防范，减少不合规事件的风险因素。

(四) 优化机构内部管理流程，明确职能和责任分工

在机构和个人双罚制的责任追究模式下，机构内部的合规制度建设和风险措施预防必不可少。随时了解数据法律动态，组织内部人员的合规培训、寻求外部中介机构支持、加强与业务和监管部门的联系和沟通、做好内部制度建设都是风险防控的必要选择。做好内部制度建设，其实也是网络安全负责人履行尽职义务的最好证明。在内部人员兼任网络安全负责人时，通过优化职能分配以减少利益冲突也是降低风险的选择之一。

(五) 外聘 DPO 职位，充分利用外部资源

《网络安全法》并未明确指出网络安全负责人是否必须由企业内部人员担任，而 GDPR 则明确规定 DPO 可以是数据控制者的员工或者外部专业机构和个人，并允许一个专业机构或个人在不产生利益冲突的情况下兼任多家企业的 DPO。在 GDPR 项下，外部 DPO 的聘请能有效避免独立性和利益冲突的风险。我们也认为，在《网络安全法》项下，允许外聘网络安全负责人，以减少企业的内部风险是可行的做法。尤其是在企业内部因资质或意愿等因素没有合适人选担任网络安全负责人的情况下，考虑聘请更具专业背景和能力的外部机构或个人不失为一个合适的可选项。

（唐文翰先生对本文亦有贡献。）

[17] 参见高富平、王文祥:《出售或提供公民个人信息入罪的边界——以侵犯公民个人信息罪所保护的法益为视角》，载《政治与法律》2017 年第 2 期。

[18] WP 243 rev.01 Guidelines on Data Protection Officers, p11.

汉坤网络安全和数据合规系列：

之一：健康医疗大数据领域的政策和法律问题

之二：《网络安全法》简评

之三：数据出境不再任性

之四：网安审查，大幕开启！

之五：个人信息保护，刑法的归刑法

之六：数据出境安全评估，操作指南来了！

之七：CII，网安法核心制度重磅落地

之八：个人信息安全的“GSP”来了！

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国法律及实务的最新动态和发展，上述有关信息不应被看作是特定事务的法律意见或法律依据，上述内容仅供参考。

如您对上述内容有任何问题或建议，请与汉坤**朱敏律师（+8621-6080 0955; min.zhu@hankunlaw.com）**联系。